JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 04, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

DESIGN A DEEP LEARNING MODEL FOR AN ENHANCED FINGERPRINT IDENTIFICATION SCHEME

Ram Kumar[1], Dr. Manoj E. Patil[2]

[1]Research Scholar(Ph.D), [2]Research Guide

[1,2] Department of Computer Science & Engineering, Dr. A.P.J Abdul Kalam University , Indore, India

[1]hr.coet@gmail.com , [2]mepatil@gmail.com

Abstract

In this research work, we analyze a new way to improve fingerprints when there is a lot of background noise. First, the image of the fingerprint is enhanced in the frequency domain, and then a binary fingerprint is made. After the second step wrongly boosts these regions, they are reassembled using a classification deep Convolution neural network with orientation selection. Both the traditional frequency domain enhancement method and the deep learning method can work together in the framework of the proposed method. To design a deep learning model for enhanced fingerprint identification, the results of the tests show that the suggested method works better than other methods.

Keywords: Fingerprint, Deep Learning, Restricted Boltzmann machine, Convolution neural network.

1. Introduction

In today's world, figuring out who someone is a significant step. To get into email or a secure building, to find out who a person or suspect is in an investigation, to make a central database of all the people in a country, and do many other things, we need systems that can quickly and accurately identify and verify people. We may see these kinds of systems in action often in the real world. Fingerprint scanners [1] on laptops both identify the user and let them use the device. In the classroom, fingerprint scanners confirm the user's identity and show who is there. It is also essential to make sure that these technologies are used safely. A fingerprint scanner in a safe place would be used for security, but not the one in the classroom. In this situation, security has a lot riding on it, which is why these systems need to be very accurate. The method chosen for identifying people takes into account both the required level of security and the kinds of techniques that can be set up technically.

1.1 Biometric Recognition

What we've seen is that modern technology needs systems that can uniquely identify a person. we can show who you are in a number of ways, such as with a password, a word from someone in charge, or even your own physical traits. People's unique physical and/or behavioral traits that can be used to identify them are called "biometric traits." When we meet new people in our daily lives, for example, we usually know them by their faces, but we may also know them by their voices. When we get a good look at someone from a distance, one of the first things we notice is how they move. So, the face, the voice, and the way a person walks are all biometric traits.

Submitted: 17/10/2022 **Accepted**: 14/11/2022

1.2 Fingerprints as Reliable Biometric Identifiers

A fingerprint is a pattern on the skin of a person's finger that is unique to that person. It has been shown that a person's fingerprints don't change much over time. If you cut or bruise your finger, the fingerprint will still be there after the injury has healed. Because of this, fingerprints are the most durable things you can find. It has also been shown that each person has unique fingerprints, making them a good choice for use as an identifier. Fingerprints have been used to identify people for more than a hundred years. Scientists have been studying fingerprints for almost a century, and in that time, they have found very few strange ones. This finding supports the idea that fingerprints should get a high score for being unique. For a long time, fingerprint-based identification and verification were mostly made by trained professionals with the right tools. That is, no computer programs could do these tasks automatically before then. Fingerprints have been used to identify people since long before computers and computer systems were widely used for identification and verification.

1.3 Fingerprint Features

From a person's fingerprints, you can tell a lot about them. Feature extraction is used a lot in fingerprint recognition tasks like enhancing, aligning, matching, and classifying. To reach these goals, having four main traits will be most helpful. This section will have a lot to say about these issues. But first, let's talk about what ridges and valleys on a fingerprint mean. Then, we'll talk about the next thing. Spaces and projections make up the basic pattern on the epidermis of a living thing. These projections can cause black lines to appear in the final fingerprint picture. Ridges are the name for these bumps. As a side note, the white color of the shot comes from the empty spaces between the ridges. We call these spaces "valleys," and they let us move on to the next step of defining fingerprint features. Here, we'll divide ridges into four groups: ridge orientation, ridge frequency, ridge singularities, and ridge behaviors. Innovations in computer science have a direct impact on the progress of fingerprint identification as an IT application. A new fingerprint identification algorithm has been made possible by advances in artificial intelligence, particularly in deep learning image processing. We classify the history of AI advancements in the fingerprint field into three distinct phases and examine the second-stage development trend. While traditional fingerprint recognition methods relied on minute details, the new deep learning-based [3]fingerprint identification technology uses image features for identification. This research looks into the typical modes of use and methods typically employed by deep learning systems for fingerprint identification, provides a foundational set of technical schemes built on top of this technology, and proposes several foundational methods and techniques like image processing and dimensionality reduction. Models of DNN [4] already in use, such as the convolutional neural network and the auto-encoder network, are presented and discussed for their potential use in fingerprint recognition. The outcomes demonstrate that, across many metrics, the AI fingerprint identification algorithm outperforms its traditional counterpart.

2. Related work

Abdulkader, Zaid et al.(2022) Fingerprints are often used for large-scale security systems because they are so accurate. When used in smartphones, they have helped with both security and money transfers. This article shows a new way to recognize fingerprints by using ridge and valley patterns that are natural to fingerprint photos. By rotating Gaussian semi-filters, these characteristics were taken out. This fingerprinting method is very clever because it combines directional filters with different kinds of Gaussian filters. We are given a high-tech ridge/valley detector that lets us find ridges and valleys with pinpoint accuracy.

Alotaibi, Nouf et al.(2020): In this study, a brand-new way is found to improve the quality of fingerprints even when there is a lot of background noise. First, Gabor filters are used to improve the image of the fingerprint. Then, local adaptive thresholds are used to make a binary fingerprint. In the second step, classification deep Boltzmann machines (DBMs) with a range pattern from the first step are used to rebuild these areas that were wrongly improved in the first step. The proposed solution uses the usual strategy for improvement, which is based on Gabor filtering and deep learning, and makes each of them better. The Biometrika, Italdata, Crossmatch, and Swipe databases, and the FVC 2004 database, were made in many different ways. Experiments have shown that the method suggested improves the performance of fingerprints and gives better results than other methods.

Rema, N. R.,et al.(2021) If you need to compress a fingerprint image so that it can be used for fingerprint recognition, you should use the fastest method that still gives you a high-quality image. Only up to a compression ratio of 180:1 can the techniques in the literature guarantee a 100% recognition rate. Any system for identifying people will be affected by how photos are compressed. This study suggests a multiwavelet-based identification method to improve identification accuracy even when images are very compressed. The SA4 (Symmetric Antisymmetric) multiwavelet uses both the decimated and undecimated coefficients as ways to tell them apart. The multiwavelet transform's ability to identify things is looked at using wavelet and multiwavelet compressed images of different sizes.

Seekoti et al. (2022) The user enters a personal identification number (PIN) into an ATM after inserting a card with their name and other information on it. The customer's PIN and the reference PIN, which have both been saved in the bank's Server, are compared. After three wrong PIN entries, the customer's ATM card will be turned off temporarily. The customer will have to go to the bank and fill out some paperwork to reactivate the card, which will likely take some time. Biometrics like fingerprints have been used to make these kinds of mistakes less likely.

SENG et al(2018) This work gives a multi-view fingerprint image acquisition method and a matching identification algorithm based on the fingerprint direction field. This is done to fix problems with traditional fingerprint collection methods, such as image distortion, alignment problems, and low resolution. There can be problems with deformation, alignment, and not enough resolution. The multi-view fingerprint acquisition method can get many fingerprint images at once and may prevent fingerprint images from getting distorted. In this method, the correctness and likelihood of a single fingerprint match are given the most weight. The

proposed matching recognition method was also compared to the industry-standard algorithm for fingerprint recognition.

3. Methodology

Overview of Framework

the two main steps of the proposed method make up its framework:
1) matching fingerprints and processing them to make the necessary tensors, and
2) using a hybrid deep neural network to model the relationships between pairs. In particular, when comparing a latent fingerprint to a reference fingerprint, it is common to run both fingerprints through several preprocessing steps.

In these steps, enhancement, segmentation, estimating the RBM (Restricted Boltzmann machine), and coarse alignment are often used. This fits with the way things are usually done when getting ready. During preprocessing, an orientation field tensor (OFT) and a fingerprint image tensor CNN are made (OFT). These tensors were made by analyzing two fingerprint pictures and their orientation fields, which were then added together. A deep hybrid network[6] is made up of many CNNs, and an RBM models the pair-relationship from multi-scale and multi-type patches of the CNNs and an RBM to determine whether two fingerprints are a match. In a network, all of the nodes are trained and optimized at the same time.

Preprocessing

the plan for what will be done during the preprocessing phase. First, a latent fingerprint and a reference fingerprint are shown in more detail and given orientation fields based on CNNs and an RBM. Then we find similarities between the two. Then, the improved fingerprint images, the CNNs and an RBM orientation[7] fields are put through a hybrid alignment. This gives us the tensors CNNs and an RBM. Here's a quick rundown of the information:

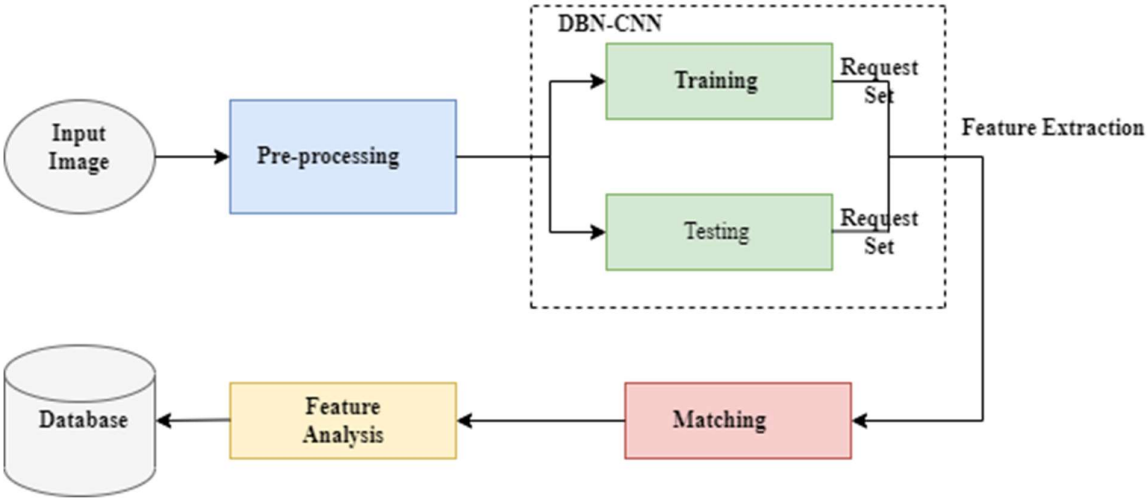

Figure 1: Proposed Framework

As a picture, the preprocessing schematic can help. Remember that, as explained, there are two ways to combine the CNNs and an RBM. This section will only show one kind of CNNs and an RBM.

Enhanced Fingerprint Image and Corresponding Orientation Field Generation

Due to their differences, the improved fingerprint photos and orientation fields for the latent and the reference fingerprint need to be done differently. Using the method described, we first make a better fingerprint image, an estimated orientation field, and a quality map for the latent fingerprint. The next step is to make the hidden fingerprint. This quality map is then used to separate the area of interest (ROI) from the fingerprint picture and the orientation field that is made from the fingerprint. Lastly, a fingerprint orientation model called Convolutional Neural Network (CNN) is used to regularise the segmented orientation field for denoising and estimating orientations for moderately dirty regions. With the RBM (Restricted Boltzmann machine) approach, you can make an improved fingerprint image, an estimated orientation field, and a segmentation of the ROI. This is done because, most of the time, the reference fingerprint is of good enough quality to be used. In the same way, the segmented orientation field of the CNNs[9] and an RBM model is made more regular by the RBM (Restricted Boltzmann machine) model. So, the latent fingerprints and the reference fingerprints[10] are improved, and the functional optical mapping Fourier transform is used to make orientation fields.

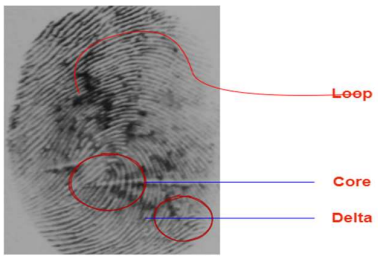

Figure 2: Indemnification

Figure 3: Data set for processing

Proposed Hybrid Deep Network

1. Starting with " there is an explanation of the deep hybrid network. Next, we'll talk about the individual pieces in the set.
2. Use the method given in to get fingerprints from images that have been improved.
3. The position changes of the alignment are shown by (x, y), and the rotation changes are indicated by.
4. There are twelve pixels on each side of the hexagon.
5. We can find the average orientation of an element by taking the average direction of all the pixels that make up the element.
6. All references to the feature vector should be understood in terms of how this element and its six neighbours are aligned.
7. A calculation called the Euclidean distance is used to figure out how similar two feature vectors are. The best 20% of all possible pairs of feature vectors are chosen.
8. The cost is calculated using the formula C(P, Q′) = P p,q′ (p, q′)/N, where Q′ is the OF that was made by transforming P to Q, p P and q ′ Q′ are the elements, p and q ′ are the average orientation of p and q ′, and N is the number of element pairs that overlap.

Convolutional Neural Network (CNN)

Normal neural networks, which were talked about in before this one[11], are similar to convolutional neural networks. Both networks are made up of neurons with weights and biases that can be changed through training. Each neuron gets data, does a dot product on that data, and then may or may not add a nonlinearity [12] to the output of that neuron. Raw picture pixels, on one end of the spectrum, and class scores, on the other, continue to be scored using a single, clear scoring function that is expressed by the network. They are similar to traditional Neural Networks in that they have a loss function (such as SVM or Softmax) on the last fully connected layer of the network, and we can still use the strategies and methods we came up with to learn these networks[13]. So, what then changes? As the name suggests, ConvNet architectures are built around the idea that the inputs are images. This lets us put certain things about the images themselves into the code. Because of this, the forward function can be set up faster, and a large amount can cut the total number of network parameters.

RBM (Restricted Boltzmann machine)

RBM is a generative stochastic artificial neural network that uses its inputs to learn how probabilities are spread out. With this distribution, it is possible to make predictions. used it to solve a classification problem by modeling [14] the joint distribution of inputs (x = (x1,..., xm)) and outputs (y = (1,..., C)) with a hidden layer of binary stochastic units (h = (x1,..., xm)). Successfully used it for a classification problem in which the joint distribution of an (h1, . . . , hH). The first thing we need to do is define what we mean by "energy function."

$$E(y, x, h) = -h^T W_X - r^T x - s^T h - t^T e_y - h^T U e_y$$

Where W and U are both weight matrices[16]. For the input x, the hidden units h and the representation e_y, r, s, and t stand for the bias weights, also called offsets. e_y= (1i=y) With the notation C i=1, y is represented as "one out of C." With the help of the following equation, you can figure out what the chances are that y and x will be:

$$p(y|x) = \frac{\exp\left(t_y + \sum_j g(s_j + U_{jy} + \sum_i W_{ji}x_i\right.}{\sum_{y*\epsilon\{1,\ldots,C\}} \exp\left(t_{y*} + \sum_j g(s_j + U_{jy*} + \sum_i W_{ji}x_i)\right)},$$
$$where\ g(.) = \log(1 + \exp(.)).$$

The proposed hybrid deep network uses the RBM to combine the results of a group of CNNs to decide whether a pair of fingerprints is real. The goal of discriminative training is to minimize the objective function L, which can be described as follows since it is done in an environment that is good for supervised learning and only needs to get a good prediction of the target based on the information given:

$$\mathcal{L}(\mathcal{T}) = \sum_{i=1}^{|\mathcal{T}|} L(x_i)$$

The loss function $L(x_i) = \log p(\frac{y_i}{x_i})$, where T = (x_i, y_i) is a representation of the training set.

Proposed hybrid approach

Here's an example of how the deep hybrid network works together to improve performance. In the first step, a set of CNN's are trained one at a time using the binary cross entropy loss. The binary types are what binary fingerprints are used to check[17]. The stochastic gradient descent algorithm, in which the gradient is found by back-propagation, is often used to reduce the loss. The CNNs are then used to train the RBM, using stochastic gradient descent to optimize its loss in the same way that the CNNs do. Since the probability is an expression with a closed form, its gradient, logp(y|x), can be calculated directly. W, U, s, and t are the important things to learn. By backpropagating errors from the RBM layer to each layer of the CNNs, the network as a whole can be fine-tuned[18]. For this tuning, the slope of the loss with respect[19] to wq is used. The expression for this is as follows:

$$\frac{\partial L}{\partial \omega_q} = \frac{\partial L}{\partial x_q}\frac{\partial x_q}{\partial \omega_q}$$

where ω_q stands for the weight value of the qth convolutional neural network[20] and x_q Stands for its prediction. A closed-form equation can be used to figure out L x_q, and CNNs' back-propagation process can be used to figure out x_q x_q.

Conclusion

We showed that gradient-calculated orientation fields can be fixed by using continuous restricted Boltzmann machines. This method was used to figure out how big these fields were. We have progressed in developing deep learning strategies for estimating the orientation field.

One of our long-term goals is to be able to do this with deep neural networks without having to make any guesses about orientation fields. With such a large collection of fingerprints, this could be a good area to study in more depth. In this research, a new way to find fingerprints that are hidden was suggested. We came up with the idea of modelling the pair relationship between two fingerprints as the similarity feature for recognition. This way, it wouldn't be necessary to separate the representation features of each fingerprint and then compare how similar they are for recognition. So, we wouldn't have to take features from each fingerprint to represent it anymore manually. With this method, decisions about matching are made based on statistical correlations between fingerprints, which give a more nuanced description of how similar they are. The deep hybrid network has been carefully created to include a set of CNNs with different sizes and architectural layouts. This is because latent fingerprints have different shapes, and some parts are dirty. Experiments with two datasets show that the proposed method is better than the current best method.

Reference

[1]. Abdulkader, Zaid A. “Fingerprint Identification System Using Half Smoothing Filters.” Webology, vol. 19, no. 1, 20 Jan. 2022, pp. 406–418, 10.14704/web/v19i1/web19029. Accessed 27 Jan. 2022.

[2]. Alotaibi, Nouf. “A New Method to Enhance Fingerprint Image Reconstruction Using Deep Boltzmann Machine.” International Journal of Intelligent Engineering and Systems, vol. 13, no. 1, 29 Feb. 2020, pp. 113–123, 10.22266/ijies2020.0229.11. Accessed 6 Sept. 2022.

[3]. “An Improved Fingerprint-Based Document Image Retrieval Using Multi-Resolution Histogram of Oriented Gradient Features.” International Journal of Engineering, vol. 35, no. 04, 2022, pp. 750–759, 10.5829/ije.2022.35.04a.15.

[4]. Rema, N. R., and P. Mythili. “Extremely High Compression and Identification of Fingerprint Images Using SA4 Multiwavelet Transform.” International Journal of Image and Graphics, 21 Jan. 2021, p. 2150037, 10.1142/s0219467821500376.

[5]. Seekoti, Sruthi. “Smart ATM Pin Recovery System Using Fingerprint Identification.” International Journal for Research in Applied Science and Engineering Technology, vol. 10, no. 6, 30 June 2022, pp. 1336–1340, 10.22214/ijraset.2022.44126.

[6]. SENG, Dewen, et al. “An Improved Fingerprint Image Matching and Multi-View Fingerprint Recognition Algorithm.” Traitement Du Signal, vol. 35, no. 3-4, 28 Dec. 2018, pp. 341–354, 10.3166/ts.35.341-354.

[7]. SENG, Dewen, et al. “An Improved Fingerprint Image Matching and Multi-View Fingerprint Recognition Algorithm.” Traitement Du Signal, vol. 35, no. 3-4, 28 Dec. 2018, pp. 341–354, 10.3166/ts.35.341-354.

[8]. Zhou, Ru, et al. “Fingerprint Identification Using SIFT-Based Minutia Descriptors and Improved All Descriptor-Pair Matching.” Sensors, vol. 13, no. 3, 6 Mar. 2013, pp. 3142–3156, 10.3390/s130303142.

[9]. Chourasia, Jaishri. "Identification and Authentication Using Visual Cryptography Based Fingerprint Watermarking over Natural Image." CSI Transactions on ICT, vol. 1, no. 4, Dec. 2013, pp. 343–348, 10.1007/s40012-013-0033-1.

[10]. "Fingerprint Reorganization Using Minutiae Based Matching for Identification and Verification." International Journal of Science and Research (IJSR), vol. 5, no. 5, 5 May 2016, pp. 1710–1715, 10.21275/v5i5.nov163751.

[11]. "Universal Identification Model of DNAFIDs: DNA Fingerprint Based Identification System." Journal of Xidian University, vol. 14, no. 5, 13 May 2020, 10.37896/jxu14.5/297.

[12]. KumarSahu, Subrat, et al. "Fingerprint Identification System Using Tree Based Matching." International Journal of Computer Applications, vol. 53, no. 10, 25 Sept. 2012, pp. 11–16, 10.5120/8455-2259.

[13]. "Fingerprint Based Authentication System Using ARM7." International Journal of Science and Research (IJSR), vol. 5, no. 5, 5 May 2016, pp. 440–443, 10.21275/v5i5.nov163297.

[14]. Moon, Daesung, et al. "Improved Cancelable Fingerprint Templates Using Minutiae-Based Functional Transform." Security and Communication Networks, May 2013, p. n/a-n/a, onlinelibrary.wiley.com/doi/10.1002/sec.788/abstract, 10.1002/sec.788.

[15]. KumarSahu, Subrat, et al. "Fingerprint Identification System Using Tree Based Matching." International Journal of Computer Applications, vol. 53, no. 10, 25 Sept. 2012, pp. 11–16, 10.5120/8455-2259.

[16]. M. A. Medina-P´erez, A. M. Moreno, M. A. F. Ballester ´ et al., "Latent fingerprint identification using deformable minutiae clustering," Neurocomputing, vol. 175, pp. 851–865, 2016.

[17]. K. Cao and A. K. Jain, "Automated latent fingerprint recognition," IEEE Trans. Pattern Anal. Mach. Intell., 2018.

[18]. K. Cao, D.-L. Nguyen, C. Tymoszek, and A. K. Jain, "End-to-end latent fingerprint search," IEEE Trans. on Information Forensics and Security, 2020.

[19]. A. Dabouei, H. Kazemi, S. M. Iranmanesh, J. Dawson et al., "ID preserving generative adversarial network for partial latent fingerprint reconstruction," in IEEE International Conference on Biometrics Theory, Applications and Systems, 2018, pp. 1–10.

[20]. C. Lin and A. Kumar, "Matching contactless and contact-based conventional fingerprint images for biometrics identification," IEEE Trans. on Image Processing, vol. 27, no. 4, pp. 2008–2021, 2018.